Biztonság és védelem az informatikában

10. gyakorlati feladat

Készítette: Baranyi Gábor
CRC7FC

2021.04.20.

Az Enigma, és az NTFS használata

Az Enigma gépek az elektromechanikus rotoros cifrázó gépek sorozata. Az első gépeket az I. világháború végén találta ki Arthur Scherbius német mérnök, és főként a kereskedelmi, diplomáciai és katonai kommunikáció védelmére használták. Az Enigma gépek egyre bonyolultabbá váltak, és a második világháború alatt a német hadsereg erőteljesen használta őket rádiójelek titkosítására.

Használhatja ezt a gépet az Enigma üzenetek titkosítására vagy visszafejtésére (az Enigma titkosítás szimmetrikus, ami azt jelenti, hogy ugyanazok a beállítások használhatók mind az üzenet titkosításához, mind a visszafejtéséhez).

Az enigma gép egy meglehetősen összetett titkosító gép, amely négy fő részből áll:

A billentyűzet

A billentyűzet a felhasználói bevitel lekérésére szolgál. Az Enigma gép egy szimmetrikus titkosító gép. Ami azt jelenti, hogy fel lehet használni egy üzenet titkosítására vagy visszafejtésére ugyanazokkal a beállításokkal. A billentyűzetet tehát a titkosítani kívánt sima szöveg vagy a visszafejteni kívánt sima szöveg megadására használják.

A billentyűzet 26 billentyűből áll az ábécé minden betűjéhez. Ez azt jelenti, hogy a titkosított üzeneteket szóközök és írásjelek nélkül fogják összekapcsolni.

Figyelje meg, hogyan kezdődik a billentyűzet QWERTZ betűkkel QWERTY helyett. Ez annak köszönhető, hogy a német nyelvben a Z betűt gyakrabban használják, mint a levelet.

A csatlakozódeszka

Miután megnyomott egy gombot a billentyűzeten, az átmegy a csatlakozódeszkán, amely biztosítja a titkosítási folyamat első szakaszát. A helyettesítő titkosítás elvein alapszik, az átültetési titkosítás egyik formáján.

A rotorok

A betűtábla után a betű sorrendben megy át a három rotoron (jobbról balra), mindegyik másképp változtatja meg az átültetési és a Caesar-rejtjel kombinációjával! Az engima M3-on három rotornyílás és öt rotor közül lehet választani. Mindegyik rotort az I-től a V-ig terjedő római számmal azonosítják. Ez az Enigma gép néhány beállítását tartalmazza: melyik rotort használja, és milyen sorrendben helyezze el. Egy kódkönyvben ezt a sorozatot IV II III néven rögzítenék (bal, közép és jobb rotor).

Az öt rotor mindegyike másképp kódolja a betűt transzpozíciós / permutációs rejtjel segítségével, és az Enigma gépben más Csengetési beállítással csatlakoztatható. Egy másik beállítás a rotorok kezdeti helyzete: Mely betűkkel állítja be az egyes rotorokat (pl. A / B / C ../ Z, amelyeket néha kódkönyvbe rögzítenek számok használatával (01 A esetében, 02 B esetén 26 Z-hez.) Ez létrehoz egy Caesar Shift-t (Caesar Cipher) .Egy Enigma gépen a három kerék elforgatásával megváltoztathatja a rotorok helyzetét.

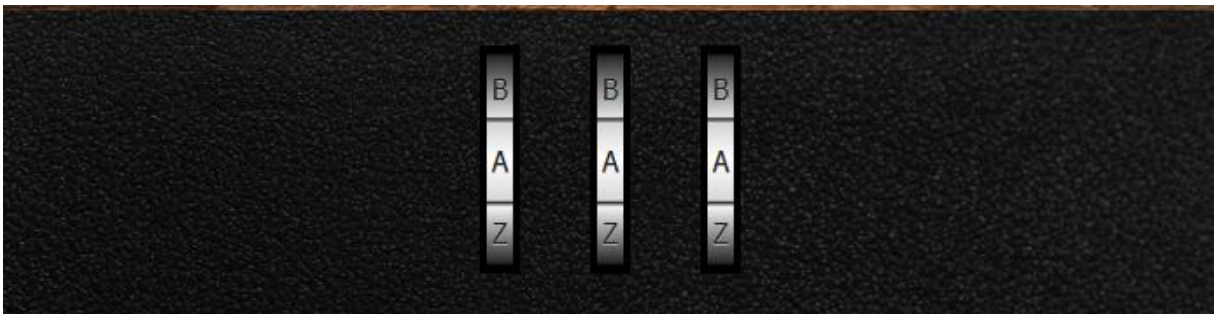
Az Enigma különböző verziói (pl. M4) négy rotort tartalmaztak, amelyek még nagyobbá tették a titkosítási folyamatot és a lehetséges beállítások számát.

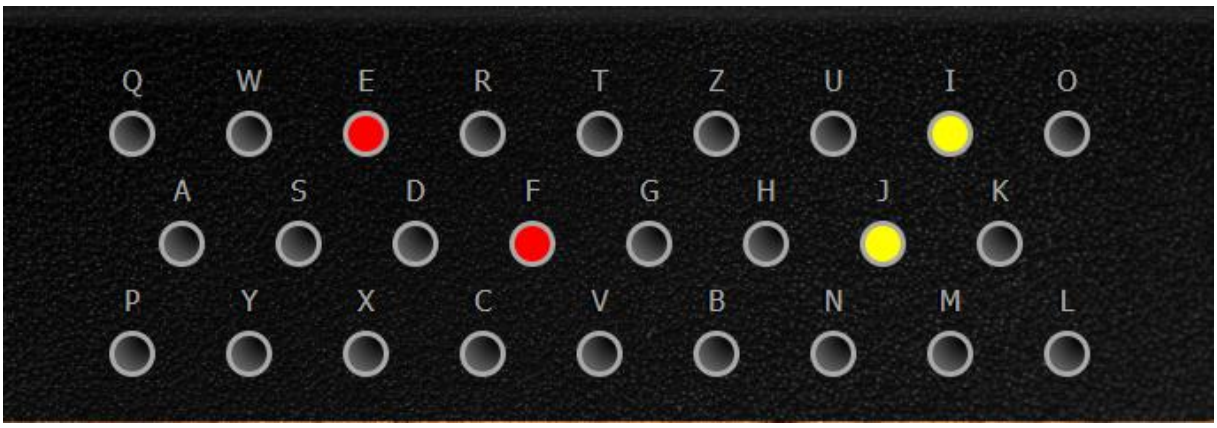
A fényvisszaverő

A reflektor egy másik típusú rotor a gép belsejében. Miután a betű átment a három rotoron jobbról balra, a reflektor visszatükrözi az elektromos áramot a rotorokon keresztül, a titkosított levelet elküldve a rotorokon balról jobbra további 3 szakaszos titkosításhoz, majd ismét a dugótáblán keresztül egy végső helyettesítő rejtjel. A reflektoron való áthaladáskor a betűre permutációs titkosítást is alkalmaznak.

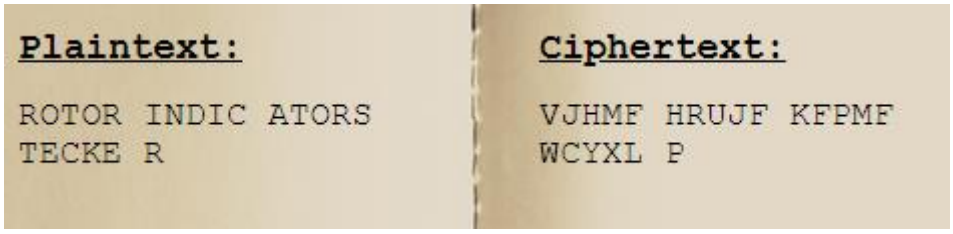
Az Enigma gépek különböző verzióinál a reflektorok különböző változatait alkalmazták. Minden reflektor más és más permutációs kódot alkalmaz. Az Enigma M3 gépeket vagy UKW-B, vagy UKW-C reflektorral szerelték fel. Ezt a két reflektort alkalmazhatja emulátorunk rotorbeállításainak ablakában.

Beállítások:





Eredmény:



Elküldtem email-ben egy társamnak a következő kódot:

CRZON JLCIA XOITH EUILH KYZNX OCBS

Beálítások:

Rotor1: a

Rotor2: b

Rotor3: c

Sikeresen dekódolta a feladatot.

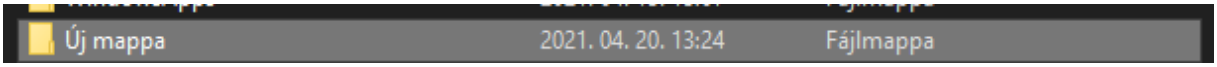
Titkosítás:

Az NTFS vagy New Technology File System (új technológiájú fájlrendszer) a Microsoft Windows NT és utódainak (Windows 2000, Windows XP, Windows 7, stb...) szabványos fájlrendszere. A korábbi Windows 95, 98(98SE), és ME nem képesek natív módon olvasni az NTFS fájlrendszert, bár léteznek programok erre a célra is.

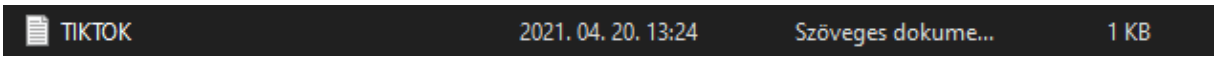
Az NTFS a Microsoft korábbi FAT fájlrendszereit váltotta le, melyet az MS-DOS és a korábbi Windows verziók esetén használtak. Az NTFS több újdonsággal rendelkezik a FAT fájlrendszerrel szemben, mint például a metaadatok támogatása, fejlettebb adatstruktúrák támogatása a sebesség, a megbízhatóság és lemezterület-felhasználás érdekében, valamint már rendelkezik hozzáférésvédelmi listával és megtalálható benne a naplózás is. Sokáig nagy hátrányaként említették a korlátozott támogatottságát a nem-Microsoft operációs rendszerek oldaláról

Titkosítás:

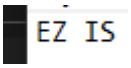
Létrehoztam egy mappát:



Bele tettem egy fájlt:

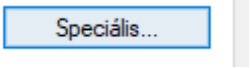


Abba írtam a következő szöveget:



Majd jobb kattintás a mappára tulajdonságok

speciális



, majd

és le Ok-olni.

Ezzel a művelettel a mappa és a teljes tartalmát le titkosítva akármit teszünk bele pluszba.

Csoport társam megnyitotta, de a fájlokat megnyitva semmit nem talált bennük.

Nem enged tömöríteni titkosított fájlokat.

Forrás:

https://www.101computing.net/enigma-machine-emulator/

https://hu.wikipedia.org/wiki/NTFS